SILICON LABS

SMART BUILDINGS

# Wireless Opportunities in a Wired Reality

## From the beginning of the building automation movement, wires have been used to connect the various parts of a building's control system. But can wireless connections now replace wires?

Today's commercial buildings are equipped with a range of building automation equipment, from heating units, fresh air units, and cooling units to lighting control, window shading, and more. The purpose of automating these utilities is to reduce the need for human interaction when regulating the indoor climate in a building, the lighting of office spaces and meeting rooms, and so on. With room-level automation, no one has to remember to adjust the temperature or turn off the lights in a meeting room when it's not being used. With the pertinent sensors and actuators distributed around the building, energy is expended precisely only where it is needed and in the required amounts.

Traditionally, all the components used in building automation have been interconnected using wires. Wired connections must adhere to various standards, such as fieldbus standards including KNX, BACnet, Modbus, and LonWorks; however, the principle is the same because each component in the system is inter-connected and each communicates via a set of wires. The simple example in Figure 1 shows a three-story house with a heating/cooling system that is fitted with building automation, which enables each floor or zone to be individually controlled.

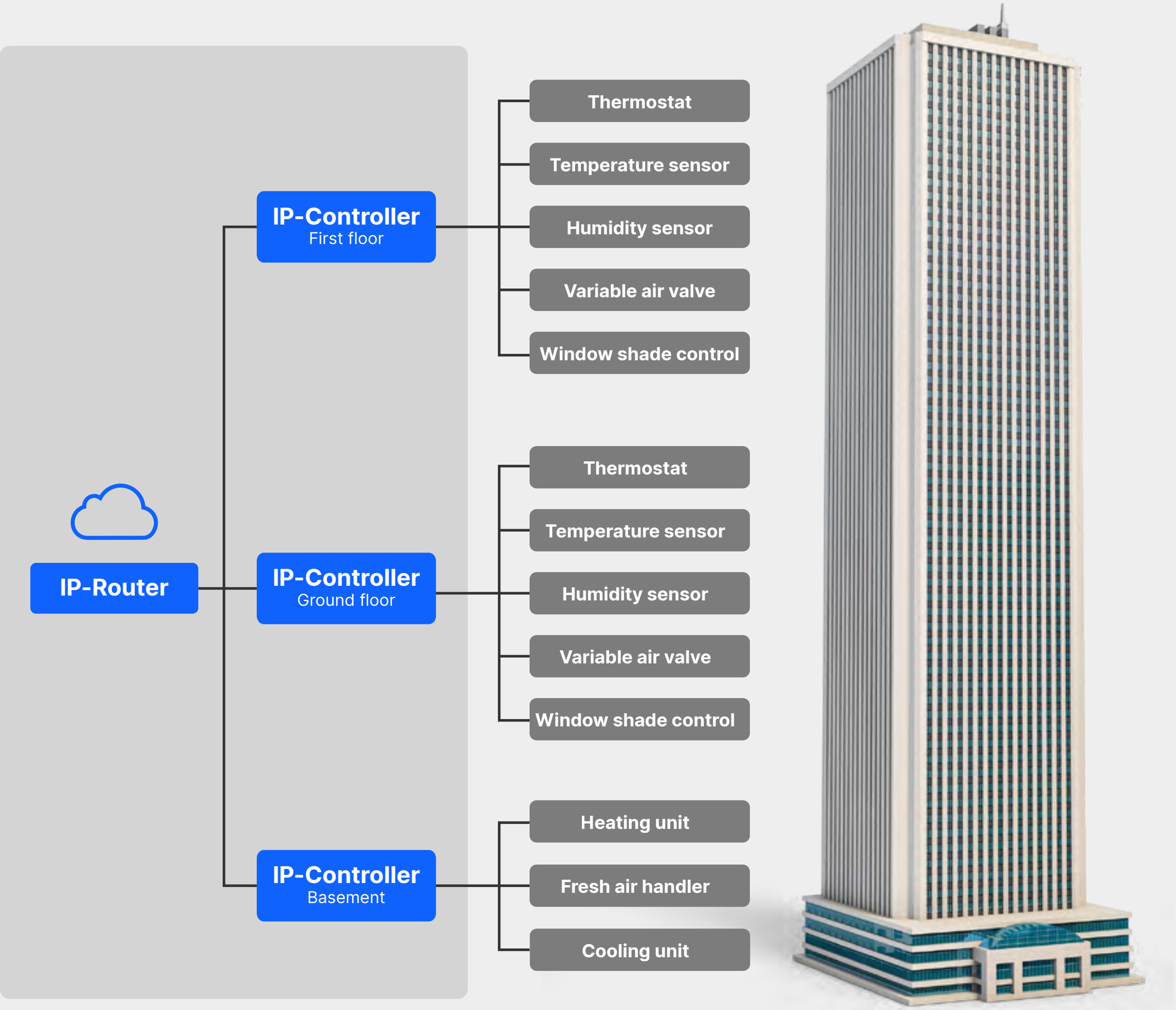
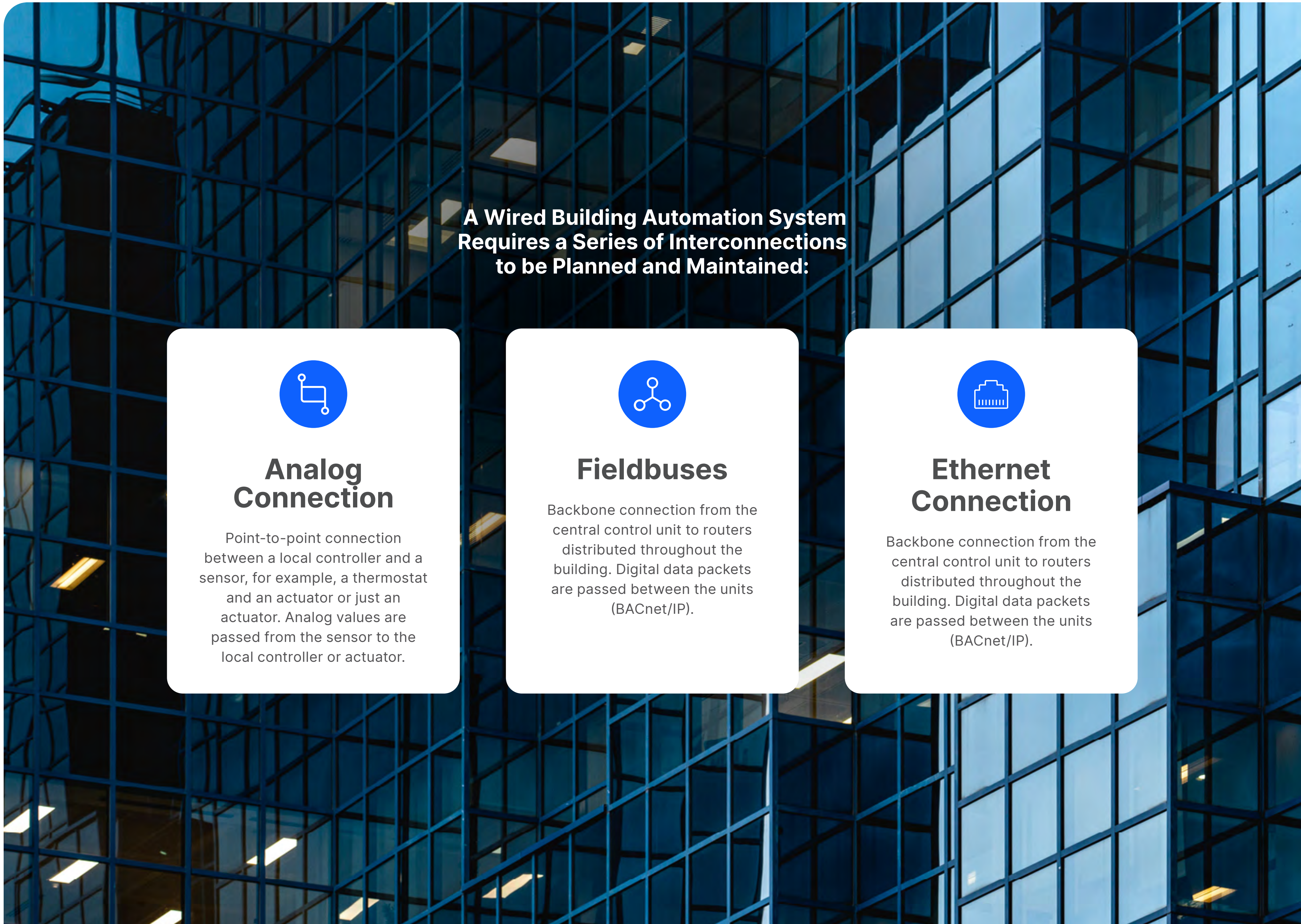


**FIGURE 1**

An example of a simple, wired building automation system

## IP Backbone

The internet-based (IP) backbone of today's systems uses an ethernet cable to communicate to an IP router housing multiple other IP controllers. In the simple topology example in Figure 1, each floor in the house has an IP controller. In the basement, where the air-handling unit is located, the fan, heating unit, and cooling unit are daisy-chained together with a fieldbus (BACnet, Modbus) to a dedicated controller. This makes it possible to control the air temperature and the air volume distributed into the ductwork of the building. The ground and first floor have their own controllers, each of which features a thermostat, zone damper, and motorized window shade interconnected using analog and digital inputs and outputs (I/O). The thermostat has two connected sensors: a temperature sensor and humidity sensor. These sensors are interconnected with a point-to-point analog connection. With this simple system, a comfortable temperature on each floor can be obtained using a set of rules configured on the central control unit. The desired temperature on each floor is set locally using dedicated thermostats on each floor, and the control unit can be used to set upper and lower limits for the temperature regulation range to ensure that the equipment in the basement can fulfill the requested room temperatures. Variable air volume (VAV) boxes regulate the amount of air to each room with their own dedicated controllers. Because the air handler delivers tempered air to pertinent VAV boxes, the speed of the fan in the air handler can be adjusted to the amount of total air volume required by each regulating VAV, thereby saving energy. Some VAV boxes contain reheat coils to regulate the humidity in the space, which is also regulated by the dedicated IP controller.



### A Wired Building Automation System Requires a Series of Interconnections to be Planned and Maintained:

### Analog Connection

Point-to-point connection between a local controller and a sensor, for example, a thermostat and an actuator or just an actuator. Analog values are passed from the sensor to the local controller or actuator.

### Fieldbuses

Backbone connection from the central control unit to routers distributed throughout the building. Digital data packets are passed between the units (BACnet/IP).

### Ethernet Connection

Backbone connection from the central control unit to routers distributed throughout the building. Digital data packets are passed between the units (BACnet/IP).

All these wires must be present in the infrastructure of the building. Right from the initial concept of the building, the wiring of the required building automation equipment must be planned and maintained. Ethernet cables and fieldbuses, not including KNX, cannot be routed in the same wire chases as high power/main power cables, so routing these cables adds costs. For analog connections, separate chases are required to avoid electrical noise and cross-talk from interfering with the signals on the analog wires. Furthermore, the restrictions on the length of the wires to use for fieldbuses and the length of the wires to use for analog connections are different, so for each run of wire from unit to unit, the length of the wire used must be carefully documented and stored to avoid exceeding the maximum wire length. Fieldbuses must be terminated, and the location of this termination per segment must be included in the documentation. The number of units connected to each segment of a fieldbus must be documented to avoid connecting too many units to each segment. When all these considerations have been planned for and drafted in the blueprints for the building, the labor of building the wire chases in the new building can start. Electricians must pull the wires — ethernet cables in some sections, fieldbuses in other sections, and the analog wires in separate chases. All wires must be labeled for easy identification. Painters and plasterers must conceal the wire chases, and, finally, building inspectors must ensure that the wires are located at the agreed upon locations and are installed according to building standards and regulations.

The next step in the creation of a wired building automation system is for a systems integrator to arrive at the job site with all the parts and mount them at their designated locations. The systems integrator may already have commissioned each part of the system beforehand (in other words, connected all the items of the system, one by one, to the control unit, named the unit, and built the logical structure of the network using a designated program). The information is stored and uploaded to the on-site controller once all the units are installed. The systems integrator may also choose to commission the units at the jobsite during the installation phase of the units. For the sensors connected with analog wires, the systems integrator must know the exact type of sensor used to correctly configure the local controller to accept the output from the sensor.

As expected, this system and the interconnection topology are “set in stone” once completed; it is built into the walls of the building structure.

### Drawbacks When Installing and Commissioning a Wired Building Automation System

1. Careful planning to ensure that wires are not too long and that segments of the fieldbuses are not overloaded and are correctly terminated.
2. Electricians to chase wires around the entire building.
3. HVAC mechanics to commission the systems to design (for example, VAV air flow together with the controls systems integrator).
4. Plasterers and painters to fix and cover the chases.
5. A systems integrator, who commissioned and installed the parts and then set up the system.
6. Extensive documentation of the work, especially items 1, 2, 3, and 5.

## The Reality of Commercial Buildings Today

Generally, wired systems are perceived as highly reliable. Once the wires have been installed, the automation units have been connected and the system has been configured, the interconnections between the components are static and stable, and the number of components is fixed. Any further changes in the wired system will require evaluation of system limitations, wiring or component adaptation, data point commissioning, and revision in controls programming and/or SCADA/visualization (the user interface).

But the reality is far from static and stable, especially for today's commercial buildings, as future conditions will dictate the following, each of which triggers a series of extensive, costly, and time-consuming work tasks. In addition, controller programming and field modifications due to changes in the building equipment and/or systems are typically not documented. These add up to the following drawbacks for wired systems:

The requirements for the utilization of the space in the building may change over time, resulting in the need to remodel the interior, move walls, repartition rooms, etc.

The development in new technology and sensor/actuator types is constant, so additional sensors/actuators with new features will be needed as time goes by.

Damage to the building structure, like water leakage, may impact the wires in the walls/ceilings/floors and cause failures in the wiring harness. A person hanging a picture on a wall may drive a nail/screw right through the wires for the building automation system. This also occurs during remodeling, when work above the ceiling and in walls can easily cut a wire or turn power off to a controller.

New building regulations for building automation (ASHRAE, etc.) will require additional actuators or sensors (for example, CO$^2$).

**Cable replanning, redesign, and documentation:** When the utilization requirements of a building change — for example, walls are added or removed — the blueprints or control drawings for the building must be reviewed to determine where all the cable chases for the existing automation equipment are routed. These cable chases must be replanned while considering the existing equipment and making sure that the new cable routes still comply with the cable-length requirements of the fieldbus and analog point-to-point connections. For this planning, the existing documentation for the system must be carefully studied to learn about the current installation and to ensure that the current equipment can handle the requirements of the new space partitioning. Once the new cable routes and room partitions are planned, electricians or systems integrators must first remove all the existing automation equipment. Then builders remodel the rooms, electricians create the new cable chases and pull the new wires to the new locations, plasterers and painters cover the cable chases, and a systems integrator reinstalls the automation equipment and recommissions it. Throughout all these steps, the existing documentation for the automation system must be updated with the new length of cable runs, new locations of terminations, and so on. However, in reality, these building renovation changes are seldom updated in the controls drawings; in fact, the as-built drawings do not include the lengths of wire runs between controllers and field devices (sensors, actuators, etc.).

**Addition of new equipment for improved performance and energy savings:** With the emergence of new types of sensors and actuators in the market that can provide a better and safer indoor environment as well as energy savings, modifications must be made to add these new devices to an existing wired automation setup. First, new wires must be installed within the sealed walls of the building structure and chased to the location of the additional device. The documentation of the existing setup, if available, must be consulted to see if that setup supports the additional load on the segment where the new device is required. Then a new cable chase must be planned for by consulting and updating building blueprints. Creating this chase will be dusty and noisy, so the room must be evacuated when electricians, mechanics, plasterers, and painters are working to build in the new cable chase from an existing sensor/actuator to the new location of the new sensor/actuator. Once the cables are in the walls, the systems integrator must ensure that the bus termination is still correctly located according to the new device, install the device, and add the device to the automation system. Once installed, the data point(s) from each new device must be commissioned and further updates on both the controls programming and SCADA platform must be made. Then all documentation must be carefully updated to reflect the new cable chases and runs, loads of the segment routers in the automation system, and the device types installed.

**Repair of damaged building structure/wiring:** Damage to the building structure that also damages the automation equipment cabling can happen anytime, but determining the origin of the damaged cable with little to no documentation can be difficult. If a point-to-point connection is damaged, and the cables are completely broken, determining the origin is easy: the signal from device X is missing, so if device X and the interface at the local controller are tested individually and proven to work, then the problem must be the interconnection between the local controller and device X. An electrician can replace the cable, and the systems integrator or the electrician can reinstall device X. But if a partially broken cable results in intermittent failures, several debugging sessions may be needed to determine whether the local controller's interface, the wires, or device X is failing.

If a daisy-chained fieldbus is damaged, depending on the type of fieldbus, devices on the entire segment may be unreachable because the damage has disconnected the required termination of the bus segment. A divide-and-test strategy must be used to determine the issue. This requires knowledge of the installed devices on the segment, including how many there are, their locations in the building, and the order in which they're connected to the bus. The technician must locate the closest device to the segment router, re-terminate the bus at the first device, and test the connection to this device. If the device is working, the cable segment from the segment router to the first device on the bus is working. The first device must be reconnected to the daisy-chained bus, and the process must be repeated for the second device. This procedure — re-terminate and test — must continue until a device that doesn't work is found. The fault in the cable is between the last tested device and the previous tested device. An electrician must replace this part of the fieldbus, and the systems integrator or electrician must reconnect all the devices on the bus again and test the segment to be sure that it works and all the devices are reachable. To complicate the debugging further, device locations are not typically documented along with the cable runs (chases) in between, so the technician not only has to divide and test but also spend time locating where to implement the divide operations.

**Updates for new standards:** New building or insurance regulations sometimes require new automation equipment to be installed in commercial buildings for the benefit of the building's users — not necessarily for the benefit of the building's owners/operators. Installing new devices in an existing building automation setup requires the same tasks to be performed as if a new device must be installed to lower energy consumption or increase comfort. Existing documentation must be studied to ensure that the local controllers can support additional devices, blueprints for the building must be consulted to plan for new cable chases, the chases must be built into the structure, and the new and required devices must be installed — just like the processes described in items 1 and 2 previously.

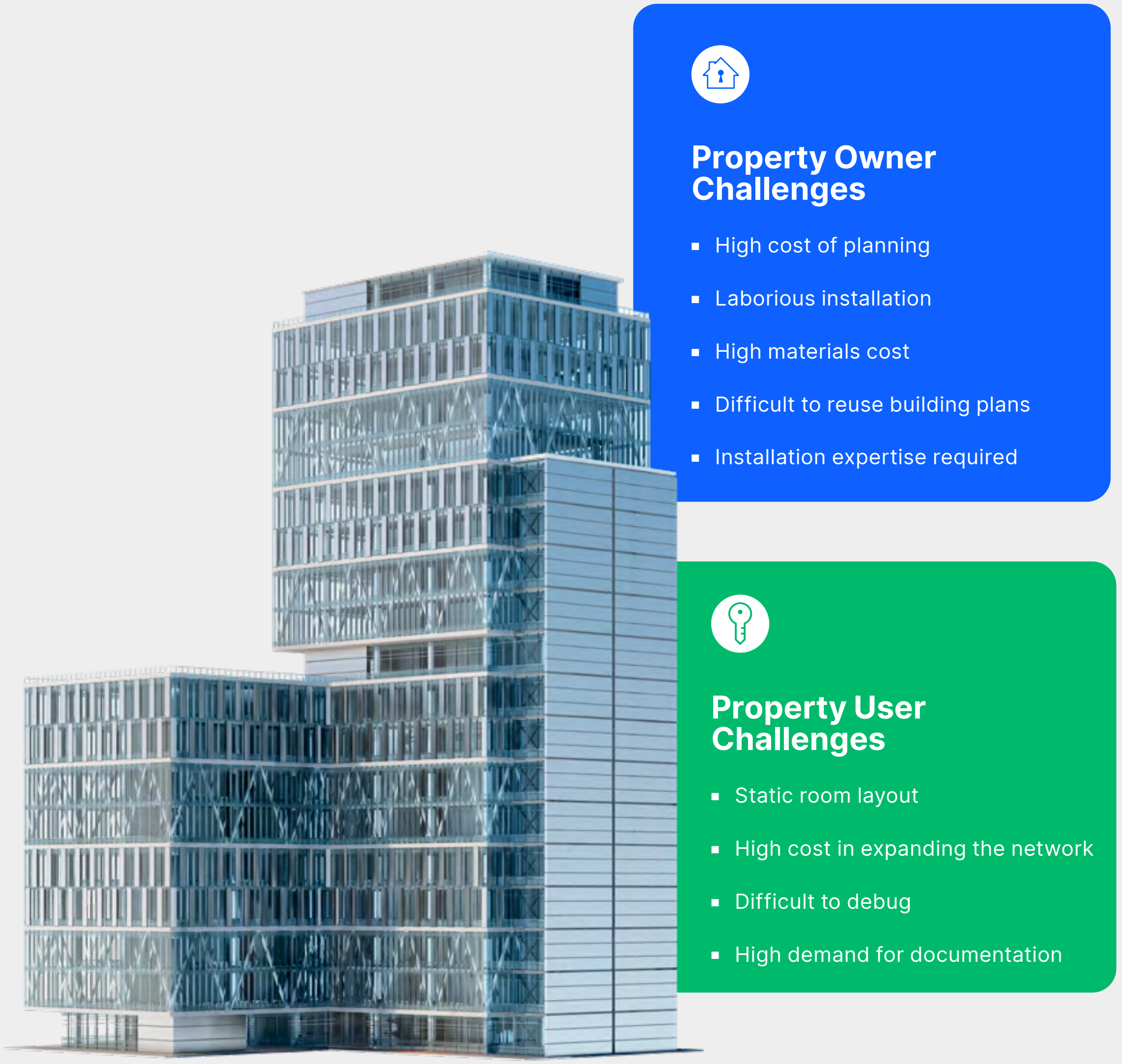
**Lack of documentation:** The latest documentation of previous work is not available.

## Factors Driving Change in Today's Commercial Buildings' Automation Systems

The need for up-to-date and precise documentation of the cable chases, device locations, and the nature of the automation system.

The involvement of many types of trade workers (electricians, mechanics, painters) whenever changes/additions/fault corrections are made to the automation system.

Disruption for the building's users whenever any changes to the existing system are required.



**Property Owner Challenges**

- High cost of planning
- Laborious installation
- High materials cost
- Difficult to reuse building plans
- Installation expertise required

**Property User Challenges**

- Static room layout
- High cost in expanding the network
- Difficult to debug
- High demand for documentation

**FIGURE 2**

Property owner and user challenges with wired connections

Wired connections also are used in HVAC and other major components of a building's automation setup.

Large and complicated parts in building automation systems, such as air handlers, furnaces, and cooling units, are often equipped with a local interface that can be used to set up the device, adjust the device, update the firmware of the device, and perform diagnostics of the device during malfunctions.

The technician typically must get close to the device, locate the connector on the device, and connect a laptop PC to the device before beginning work. If the device is an air handler in the basement of a building, this might not be an issue. But if the unit is a furnace built into the ceiling above a room in an office environment, accessing the furnace's connector requires:

- A ladder to reach the ceiling
- The evacuation of nearby surroundings and protective coverings for work areas to prevent dust from contaminating these areas
- Removal of a piece of the ceiling to expose the hidden furnace unit
- Connection to the unit with the wire from the diagnostics tool (for example, laptop PC)
- Diagnosis of and updates/adjustments to the unit
- Repair of the ceiling construction
- Cleaning of nearby surroundings to allow personnel to return to work areas

This is not only time-consuming for the technician maintaining built-in-structure devices, *it is also disruptive to the workers in the building close to the repair site.*

Outdoor mounted equipment also can be challenging to reach if a local connection with the equipment is required for updates, diagnosis, and adjustments. Large air-handling units mounted on rooftops or the side of a building can pose a hazardous work area for the technician, requiring either multiple persons to secure the worksite or the use of safety gear when approaching the unit.

Wires are also used to connect components within the building automation equipment.

For larger, more customized air distribution systems, air-handling units are often delivered in sections to a worksite and assembled at the location to allow normal trucks and cranes to handle the equipment. In these cases, the power and individual pieces of the unit must be connected for the local controller of the equipment to manage the entire assembly. As mentioned before and shown in Figure 3, a wired fieldbus is most often used for this purpose.

The previous three examples of wired connections in today's building automation industry show how wires and fieldbuses compose a trusted and proven way of interconnecting automation equipment. Because of this, the workload associated with the initial installation and with later maintenance has been accepted for so many years that it is not considered a burden — only a natural part of operating a building automation system.

But can building automation be implemented in a smarter way? Can fewer resources be used? Can greater flexibility be obtained without the cost of installing new wires?

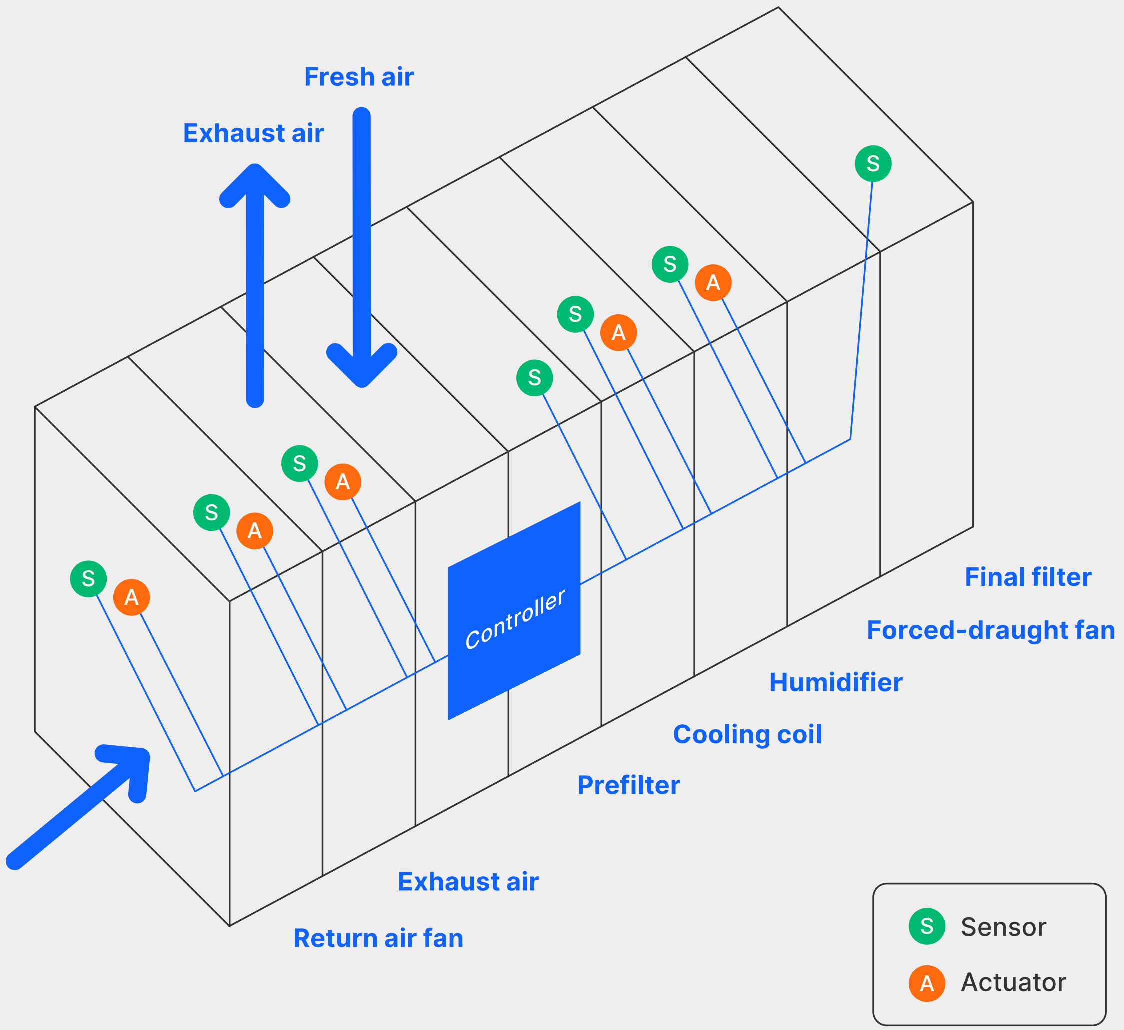


FIGURE 3

Fieldbus used for intradevice connections

## Going Wireless with Building Automation Systems

Returning to the simple setup shown in Figure 1, the three-story house with an automated indoor climate system uses wires as interconnections between the parts of the system. How can this setup be simplified? The system must work equally well on all three floors, and all the system parts must securely receive and transmit commands to measure and adjust the air volume, temperature, and amount of fresh air for each floor in the house.

One way to simplify is removing the wired interconnections on each floor and leaving the ethernet interconnection between the floors as a backbone (see Figure 4 to the right).

All the wired fieldbuses and analog wires used on each floor are replaced with wireless connections, which are labeled with small antenna symbols. The connections from the devices on each floor to the central controller are created using gateways on each floor. These gateways securely “translate” commands from the wired ethernet to the wireless field device connections on each floor.

But how can wireless connections replace wired connections? It depends on the type of wireless connections replacing the wires.

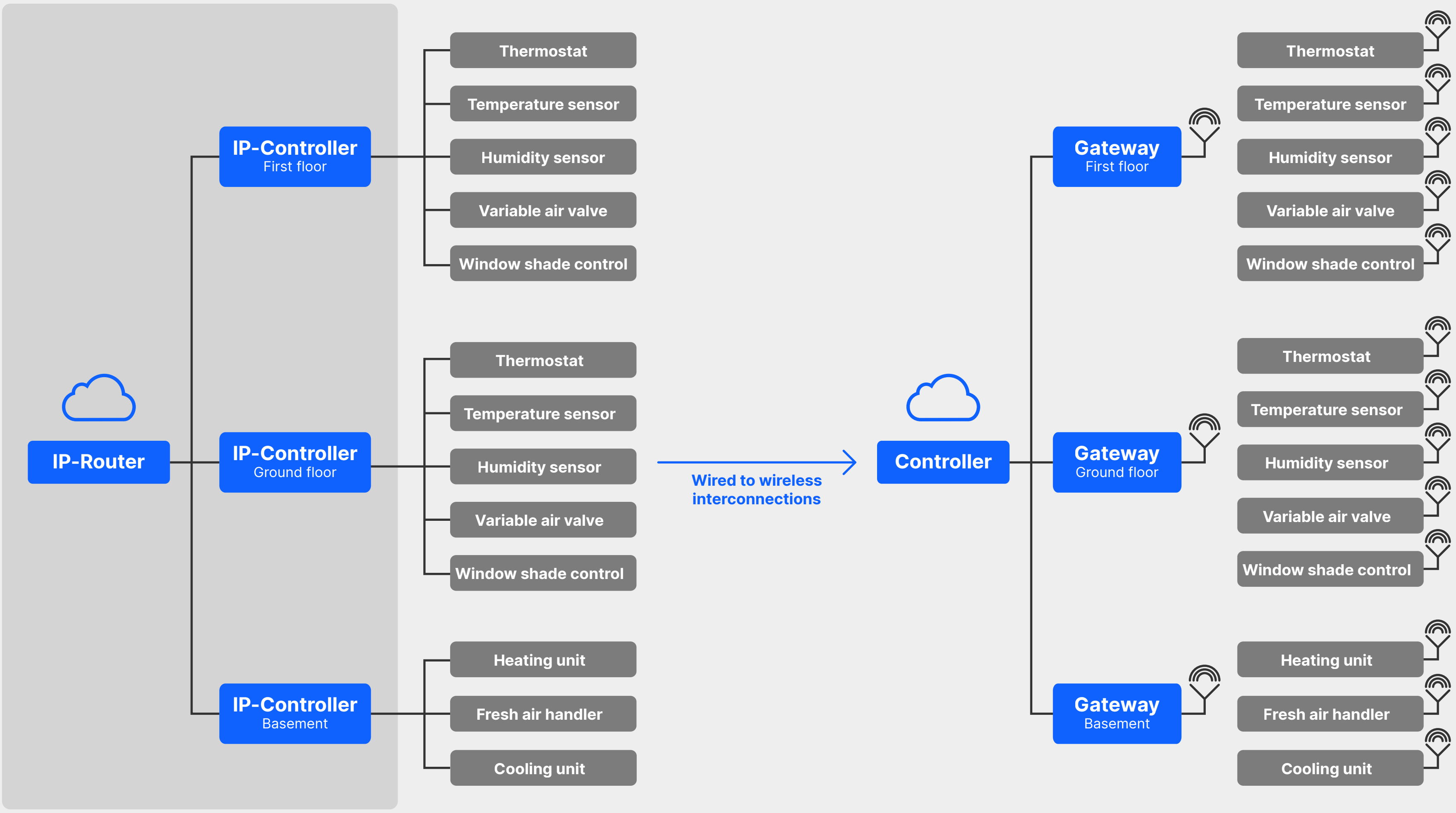


**FIGURE 4**

Wired-to-wireless transformation of a building automation system

To link two units in a network securely and reliably, the message communicated between the units is "guaranteed" to arrive at the destination through two important features of a wireless protocol:

1 Acknowledgement of all transmitted messages
2 Mesh network technology

The first item, acknowledgement, means that the sender of a message receives an acknowledgement from the receiver that the transmitted message reached its destination. This implies that the radios involved are two-way radios capable of transmitting and receiving digital messages between each other.

The second item, the mesh network technology, means that participants of a network can help each other pass on messages between devices, even if the devices are outside direct radio reach.

In Figure 5, four devices form a network, and device A must transmit a message to device C. Unfortunately, device C is out of reach, but because the devices are part of a mesh network, devices B and D can help device A retransmit the message to device C. This ensures that a connection between devices A and C is established even though the two devices cannot communicate directly with each other. And because all messages between the devices are acknowledged, device A knows that its message did reach device C. If, for some reason, the message from A to C does not pass through the network, for example, because of radio noise or because device C is broken, device A can try to retransmit the message after a while. The protocol governing the message flow between the devices will keep trying to deliver the message to device C until a certain limit of attempts is met. When this limit is reached, device A knows that device C is out of reach/order and flags this through its application to a controller/gateway in the system. This informs the operator that device C is out of order.

So, with mesh technology, multiple communication attempts and message routes through a network are tried to ensure that messages reach their destinations. This greatly improves the reliability of network communication. In fact, including more devices in a network helps the other devices deliver messages and increases the reliability of a network even further.

In addition to network reliability, network security, or the prevention of unwanted and malicious messages from corrupting the network and gaining unauthorized control over devices, is important. All modern wireless mesh networks incorporate security as a native part of their RF protocols. This security prevents any outsiders from reading the messages passing between devices. It also prevents replay attacks, which are attacks during which messages are recorded and replayed to obtain a certain response from the devices. Mesh networks prevent their messages from being read using encrypted messages and sequence counters. The content of these messages is encrypted in such a way that only the controllers and the end device can read and understand the message. If a network uses sequence counters, it assigns each new message between any device a number, and this number can be used only one time. Messages received with an outdated number are rejected.

In the wireless network shown in Figure 4, all the devices are part of the same mesh network. The devices can help each other pass on messages — no matter which floor they're on — if the RF environment permits it. Also, the route of the message through the network is not important. What matters is that the message reaches its end destination and that the transmitter of the message receives a confirmation that the message reached its end destination.

What about the power supply of a device when the fieldbuses and wires are removed? For most actuators, a local mains supply (230V or 120V) is required in the panel to transform the voltage down to 24VDC/VAC to operate the actuator. Supplying a radio transceiver is not an issue because low-voltage power is constantly available for the actuator anyway. But what about the sensors in the system? The temperature sensor and the humidity sensor in the given example must be either battery operated or 24V power operated. *Given the recent developments both in battery technology with large-capacity, small-dimension lithium-ion batteries and in radio chips with low power-down currents and high-efficiency supply circuits, a long-lasting battery solution can be implemented. If designed with the latest energy-harvesting technologies, for example, using indoor light as a source of energy, the batteries in these devices last the lifespan of the product without needing to be replaced.*

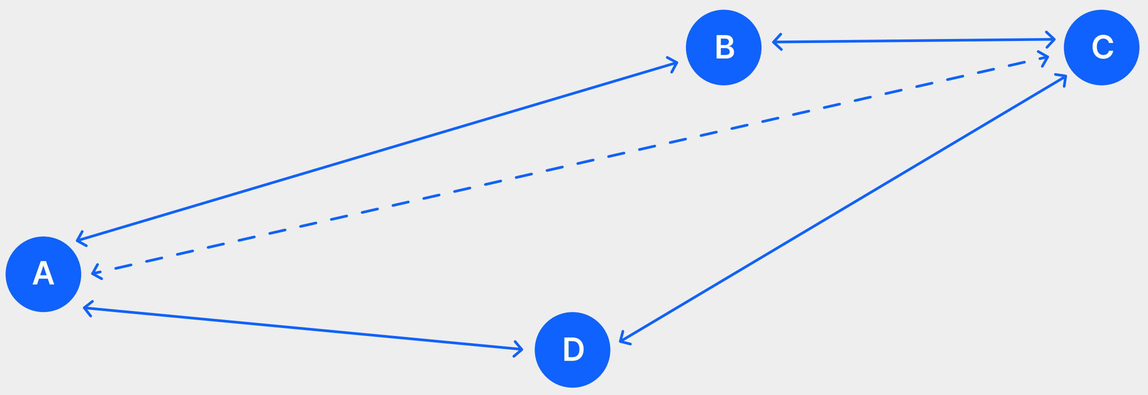


**FIGURE 5**

**Mesh network topology**

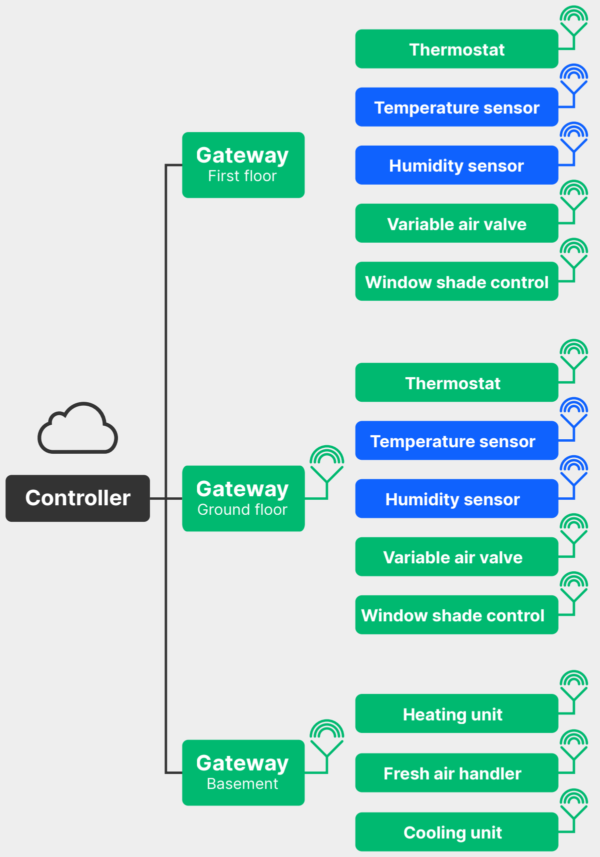


**FIGURE 6**

**Constant-powered green devices and battery-powered blue devices**

A battery-operated device is mostly in a low-current-consumption sleep state. The device periodically wakes up to sample the environment and transmits a message only when required. Such battery-operated devices cannot participate in a mesh network's message routing because they are usually in a powered-down state with a turned-off radio. The actual message routing is performed only by constant-powered devices like actuators and gateways. But messages from a sleeping device are still routed through the network by the constant-powered devices, and, when transmitting, the sleeping devices will stay awake and retransmit until an acknowledgement is received from the end-destination device.

Keeping this concept of constant-powered and sleeping devices in mind, the example shown in Figure 4 can be redrawn to show the power state of each component (see Figure 6 to the left).

All devices except for the temperature and humidity sensors are connected to a local power source, so the heating unit, the window shade controllers, the VAVs, and so on are always powered by 24V and their radios are always on and ready to receive and transmit messages. The sensors, on the other hand, are battery powered; they stay in a powered-down state until a message needs to be transmitted. When to transmit a message depends on the implementation of the application: It could be a transmission of the sensor state every fifth minute or when a threshold is exceeded. When a battery-operated device awakes and transmits a message, the mains-powered devices receive the message and retransmit it if needed. The battery-operated device stays awake until it receives an acknowledgement from the end-destination device and then enters a powered-down state again to preserve energy.

The amount of effort needed to implement the building automation system shown in Figure 6 compared with the original wired system in Figure 1 is significantly smaller:

| | WIRED NETWORK | WIRELESS NETWORK |
|---|---|---|
| 1 | Careful planning to ensure that wires are not too long and fieldbus segments are not overloaded or incorrectly terminated; planning for the construction of wire chases between each device in the network | Careful planning to ensure radio connectivity between the parts of the network; insertion of a constant-powered RF repeater in the network to bridge possible RF gaps if distances are too large |
| 2 | Electricians to install and chase wires throughout the entire building | Planning for only backbone cabling |
| 3 | Plasterers and painters to fix and cover the chases | Repairs for only backbone chases |
| 4 | Systems integrator to commission and install the parts and then set up the system | Systems integrator to commission and install the parts and then set up the system |
| 5 | Extensive documentation of the work, especially items 1, 2, and 4 | Much less documentation burden for items 1 and 2 |

In addition, the savings are significant with less chase installation throughout the building structure. No chase planning, documenting, or installing, which involves several types of experts, saves resources and time.

What about the five situations described earlier that require either changes to the topology of the automation system or repairs, debugging, or expansion of the automation system?

1 New room utilization
2 New devices added to network
3 Damage to the building structure/wiring
4 New requirements for building automation involving additional actuators/sensors
5 Lack of documentation

What is the workload for handling each of the above situations if the automation system is based on wireless devices?

## Going Wireless Makes Planning, Design, Daily Maintenance, and Troubleshooting Easy

1 Since the devices are no longer interconnected physically with each other via wires chased in the building structure, changing the location of walls or adding new walls does not require any new wire chases to be planned or constructed. The local power supply must be restored or rebuilt, but new wire chases are no longer needed. Battery-operated sensors can be dismounted and moved to new locations with little effort, and power-supplied actuators can be moved with the reestablishment of a new local power connection, but new wire chases to other devices in the building to reconnect, for example, a fieldbus, are not required.

2 Adding a new device to a wireless network does not involve the same level of planning as adding a new device to a wired network because only an eventual local power supply must be established. Wire load and segment size as well as the locations of wire chases and bus terminations are no longer needed because the devices are interconnected with the mesh network wireless connection.

3 If new legislation mandates the addition of new devices to an existing wireless network, the new devices can be installed easily because no wired connections to existing equipment are required. The new devices can be installed at the required locations. An eventual local power supply must be established, but that is all. Building new wire chases from existing equipment to new equipment, replanning bus terminations and wire loads, updating wire lengths, etc., are no longer needed.

4 Damage in the building structure affecting a part of the building automation system is much easier to locate and repair. Since the parts of the wireless building automation network are not connected through wires, they are independent of each other. Therefore, if water ingress, or leakage, affects a constant-powered actuator, only that actuator does not work. Inputs/outputs from that actuator are missing, but inputs/outputs from the other parts of the automation system are still visible for the network. And repairing the faulty device does not affect the other devices because they are not physically interconnected with each other via analog wires or fieldbuses.

In addition, the risk of a person driving a nail/screw through an important wire for the building automation system is significantly reduced since the only wires used in a wireless system are local power supply wires for actuators or constant-powered network components. No fieldbus wires or analog wires crisscross the building structures. The disconnection of a local power supply affects only one device, and since this device no longer reports to/is reachable from the network, determining whether the device is faulty is easier.

5 Documentation of where devices are located in each room is still needed, but the work required to track that compared with documenting wire chases is far less.

Compared with a wired network, the planning, construction, daily maintenance, and troubleshooting of wireless networks require far less effort during the initial installation phase because each component is independent of the other components in the network. If a wireless component stops to transmit, it is not because another part of the network is broken. It is because the device no longer transmitting is broken. With the fieldbus example, if a device stops working, the entire fieldbus segment is likely affected, so each device and wire segment of that fieldbus must be debugged until the faulty fieldbus wire segment or the faulty device is identified, and then it must be repaired. If the wires are faulty, they must be replaced with new wires. For wireless networks, the faulty wireless device must be replaced or the batteries of the device must be replaced, but that requires much less effort and time compared with debugging and repairing the fieldbus counterpart.

If the wired interface for local interconnection with a device, for example, a hard-to-reach furnace built in the ceiling structure of an office, is replaced with a wireless interface, the effort to interconnect with that furnace for debugging can be reduced by five steps (see right).

Perhaps the most important factor when comparing the two workflows is that the impact on the areas close to the worksite using a wireless connection is reduced to an absolute minimum — the presence of a technician. And the technician does not have to climb a ladder, work at abnormal heights, be exposed to dust, or expose the environment to dust. A wireless connection to the built-in device allows for a noninvasive workflow, which benefits the technician and the area surrounding the built-in device.

## Wired Building Automation Implies a Heavy Workload

| | WIRED NETWORK | WIRELESS NETWORK |
|---|---|---|
| 1 | The technician requires a ladder to reach the ceiling | Not needed |
| 2 | The nearby surroundings (furniture, equipment, wall hangings, etc.) need to be removed from personal and work areas and the remaining items need to be covered to prevent dust from contaminating them | Not needed |
| 3 | The technician must take down a piece of the ceiling to access the hidden unit | Not needed |
| 4 | The unit must connect to a diagnosing device via a wire; this may require multiple technicians and/or safety equipment | The unit can connect to a diagnosing device wirelessly while technician stands on floor |
| 5 | Update/diagnose/adjust the unit | Update/diagnose/adjust the unit |
| 6 | Ceiling repair is required | Not needed |
| 7 | The cleaning of nearby surroundings to allow personnel to return to their work seats is required | Not needed |

### Uncover the Silicon Labs Wireless Solutions for Smart Buildings

Learn More

The same benefits apply to devices in other hard-to-reach locations such as rooftops or the sides of buildings. With a wireless connection to the device, the technician does not have to be within arm's reach of the device to connect with it. The technician can remain in a safer work location while interacting with the device.

The third of the three wired use cases in building automation is the intraconnections in large and heavy equipment such as air-handling units. In this equipment, the internal fieldbus wires that must be interconnected for each component can be replaced with a wireless connection:

Power must still be connected to the individual components of the assembly, but the control wires are replaced with wireless connections. This allows for the previously mentioned wireless local connectivity feature. Again, the installation has been simplified by omitting the need to interconnect wires.

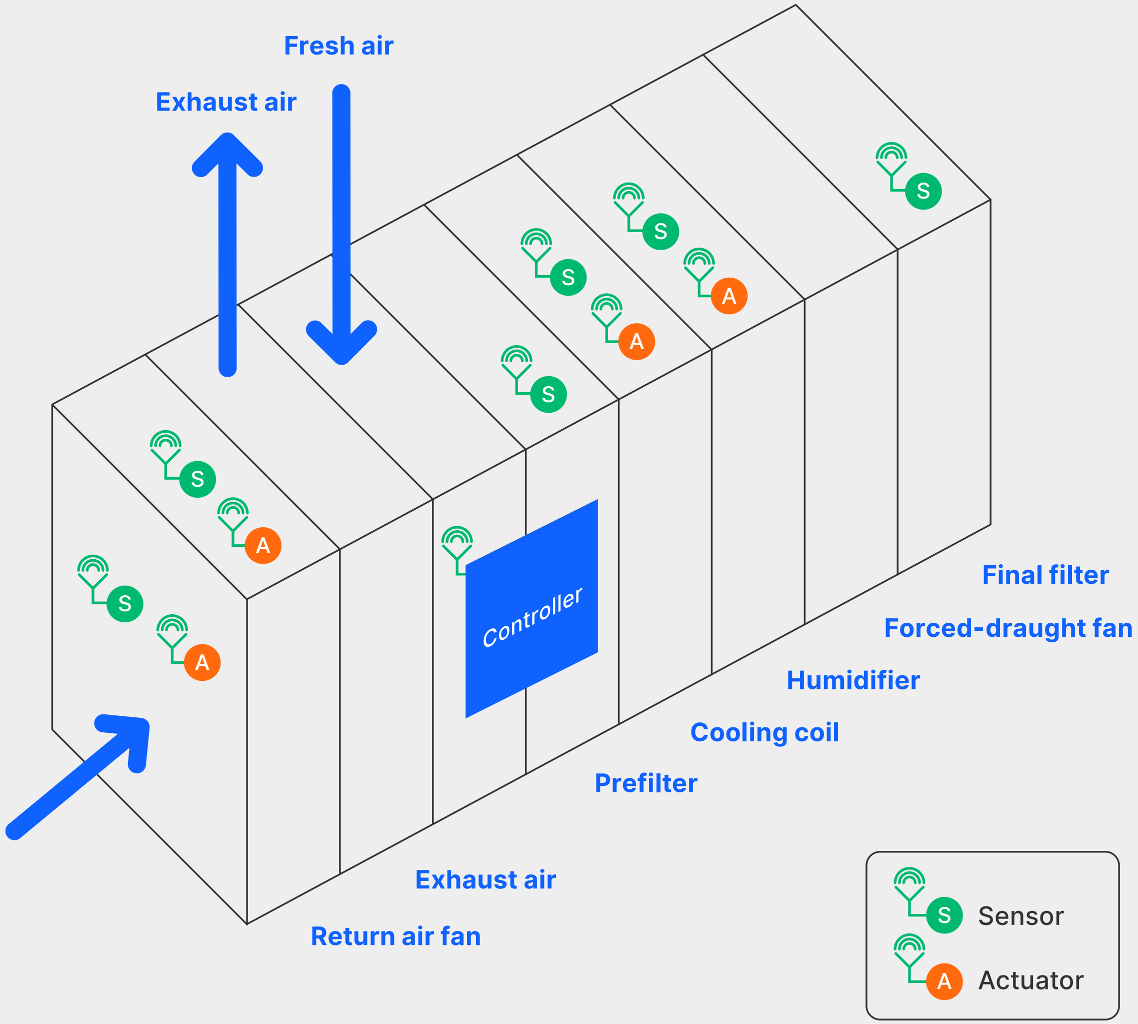


**FIGURE 7**

Wireless intraconnected equipment components

## Wireless Building Automation Installation and System Considerations

In the previous sections, the considerations, planning tasks, and workload associated with a wired installation were described and compared with that of a wireless installation. But what about the system considerations for planning, designing, and configuring a wireless network? Don't wireless networks require those as well?

For the installation of any complex system, a certain amount of planning is required. This is also true for a wireless building automation system.

The planning of a wired system revolves around wire lengths, wire-chase locations, segment loads, and locations of bus terminations, the planning of a wireless system revolves around range — the range between the individual parts (that is, devices) of the system. In wireless technology, range is not the physical distance between the devices of the system. Range is defined as the distance between the components of the system where stable radio communication between the components is ensured.

For example, two wireless devices 1 meter apart from each other may not be within each other's range if the devices are separated by a metal wall. Or two wireless devices can be 50 meters apart from each other and still be within range if they are in a hallway.

Another consideration when planning a wireless network is the ratio between constant-powered devices and battery-operated devices in the wireless network. As mentioned in the previous sections, battery-operated devices cannot pass on messages for other members of the network; *message routing is possible only through constant-powered devices*.

To ensure that all devices in a large installation of battery-operated devices and a very small number of constant-powered devices scattered across a large area can communicate with each other, a constant-powered repeater in low-range areas (that is, dead spots) needs to be installed. A repeater passes on messages from all areas of the room (figure 8 to the right).

In Scenario A of Figure 8, three of the four battery-operated sensors are within radio range of the gateway, but the fourth sensor, the occupancy sensor, is out of range. Because the other devices in the network are battery operated, they cannot pass on messages from the occupancy sensor to the gateway. The solution to this problem is installing a constant-powered device as shown in Scenario B. The repeater is always powered, so it receives the messages from the occupancy sensor and passes them on to the gateway.

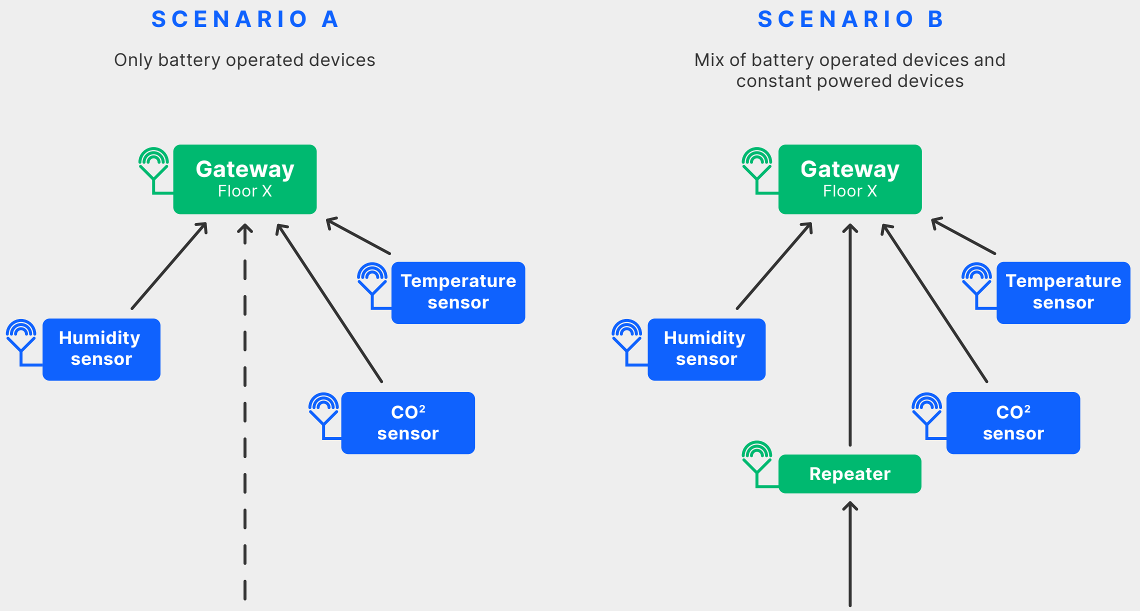


**FIGURE 8**

Ensuring range coverage in a wireless network

Another solution is relocating the gateway to operate in direct range of all the battery-powered devices.

The range of the individual devices in a wireless network depends on:

## Key Factors Impacting the Wireless Range in a Building

### The construction materials used in the building

### The RF output power of wireless devices

### The RF frequency of the wireless devices

### The antenna of the wireless devices

Each of the above four items presents the following considerations:

1 The radiation of RF energy from an antenna is like the emission of light from a light bulb. Some materials are transparent and let the light shine through with little or no loss; other materials are tinted or lightproof and attenuate or block the light. The same is true for RF energy: metals and thick, rebar-enforced concrete walls block or attenuate the RF energy, but light walls of wood or gypsum sheets are transparent and lightly attenuate the RF energy.
2 Generally, the more energy a radio outputs, the longer the range for the radio, in terms of both direct range and energy being reflected by the surroundings. So, the radio can reach corners of a room out of direct range.
3 Generally, lower-frequency RF energy penetrates objects better than high-frequency RF energy, which is more prone to reflect off the surface of objects.
4 The antenna of a wireless product is the most important part of a wireless product. With a poorly designed antenna, the range of the product is short. This means repeaters are required to pass on the messages from and to the product.

In some cases, like in open warehouses or open office spaces with very few walls, no repeaters are required to ensure a stable communication between the parts of a wireless network. But in other cases, like buildings with many rooms and “solid” walls, a couple of repeaters need to be installed on each floor to ensure stable wireless communication. The cost of installing an extra repeater or two is far less than the cost of crisscrossing a building structure with wire chases.

## Added Benefits of Going Wireless

Going wireless presents benefits in addition to the lack of wired infrastructure; the much easier installation, configuration, and debugging of devices; the requirements for less documentation because building constructions are not affected during installations or modifications; and the inherent security of the RF protocols that prevent hackers from reading messages or injecting messages into the network.

One often overlooked complication of wired systems is the commissioning of the devices in the building automation network. For a network to work properly, the devices in the network must be aware that they are part of a group of devices allowed to communicate with each other. So, each piece of equipment must be connected to the main controller of the network; receive an identification address and perhaps an alias/descriptor, for example, Second Floor, Room B, Thermostat; and then be labeled correctly to ensure that the systems integrator mounts this device in room B on the second floor.

An alternative approach to the commissioning is to mount the devices one after the other and commission the device in the field during the installation.

A third method is to buy and install precommissioned devices for which the manufacturer has previously performed all the commissioning. As with the first approach, this requires a good level of documentation to be sure that the correct devices are mounted according to the plans and device descriptions.

Wireless devices also require commissioning to be part of a network; however, each wireless device does not have to be connected to a fieldbus to be commissioned.

A wireless device can be added to a network using two fundamental methods:

1 The device can be added to a network by pressing a button on the device that forces the device to transmit a message like, “Please include me in your network.” This message is picked up by the network controller, which then incorporates the device into the network.
2 The device features a built-in identification number that is on the controller’s commissioning list. When the device awakes for the first time and requests to be added to the network, the controller recognizes the device from its list and automatically incorporates the device into the network.

Both the methods above are easier to perform compared with the wired method. No fieldbus wires must be connected or disconnected — only power needs to be connected.

Another advantage of going wireless compared with using fieldbuses is the data rate. The data rate of a powerline-based KNX link is 1200 bit/second, and if the KNX link is twisted pair, the data rate is 9600 bit/second. The ethernet backbones can operate at gigabits per second, but, as with a chain, the strength of the chain is only as strong as its weakest link, and the total network speed is set by the slowest links in the wired network, which are the fieldbuses. For comparison, the Zigbee wireless standard operates at data rates of 250,000 bit/second.

Network size or, to be more precise, segment size is another concern. Fieldbuses like KNX support only up to 64 devices per segment. A network can be larger and contain more devices, but then more segments must be added to the network. This limit of segment size and wire length for each segment means that a wired network must be carefully documented and the documentation must always be updated to ensure that the number of devices does not exceed the segment limit. A wireless network can control more than 64 devices. Again, compared with the Zigbee standard, several hundreds of devices can be members of the same network, and networks can operate in parallel if needed.

Wireless products do not require their controllers to be configured with the type of analog sensor an input port is connected to. The sensor is an individual device, and the sensed values are transmitted as digital values to other devices, for example, a thermostat. This means that thermostats no longer need to be configured according to which type of sensor is connected to the thermostat. Further, wire polarity is no longer an issue for the analog wired connections because these wired connections are replaced with a wireless link. This is another example of the simplification that going wireless offers.

## Wireless Disadvantages

To claim that going wireless compared with wired networks is effortless and challenge-free would not be accurate. This section outlines the challenges of wireless networks and ways they can be minimized.

## Wireless Building Automation is not Challenge-free

### Antenna design considerations

If the antenna is not correctly placed inside the product or is not suited for the frequency band selected, the product performs poorly. Going wireless means understanding that the antenna is the most critical part of the design. With a good antenna design, all the energy allowed to transmit is radiated in the air to be received by the other members of the wireless network and vice versa. The product can receive signals from other network members. With a bad antenna design, the range of the product is not optimal, and repeaters may be required to achieve a stable radio link.

### Indoor range estimation

Predicting the range between two radios in an indoor environment can be difficult due to building materials, local RF noise sources, and RF multipath fading, during which RF reflections on the interior create radio-dead spots in a room and influence the RF environment. This impact is different from building to building.

### RF regulatory testing

Going wireless also means that the product must adhere to the local RF regulatory authorities. So the product must not only fulfill functionality expectations but also be tested by the local RF regulatory authorities to ensure it does not interfere with other radios and radio systems in a destructive way.

### Location of devices

With a wireless product, the location of the product is very important. A wireless product mounted inside a metallic cabinet offers poor range, but a wireless product mounted on the side of the metallic cabinet provides good range except from the backside of the product.

### Battery supply and replacement

To avoid wires for power supplies and create small products, most sensors are powered by batteries, and batteries need to be replaced. This is not the case with a product in a wired system that is always connected to a power source through a fieldbus or a local power supply.

## Silicon Labs Enables Smart Buildings Designs Worldwide

### Antenna design considerations

The type and location of the antenna should be prioritized when planning the design of a new wireless product. The rest of the product should be designed around the antenna to ensure that the performance of the antenna is not compromised. Once a product is designed, the performance of the antenna is difficult to change, so great care must be taken in the design stage. Silicon Labs offers RF modules with built-in antennas. If the integration directions of these modules are carefully followed, the performance of the product will be as optimal as possible. When a custom antenna is required, and the product design group does not include an RF antenna expert, consider spending a couple of hours to get an RF antenna expert to review the product design before ordering the first prototype.

### Indoor range estimation

Indoor range estimation depends on 1) the RF properties of the structural materials of the building and 2) the RF qualities of the products being installed. A conservative approach involving a shorter-than-reality range for each product as well as the addition of an always-powered repeater at strategic locations in large rooms can provide excellent RF coverage. The cost of adding a repeater is still orders of magnitude lower than the cost of running just one segment of a fieldbus with wire chases in the walls. Multipath fading can be reduced using an RF protocol with frequency agility. If the RF frequency used to communicate between devices can change, then the location of the radio-dead spots can change, too, which enables a device in a previously radio-dead spot to be included in the communication again.

### RF regulatory testing

Silicon Labs offers precertified RF modules as well as templates that show how to get a product certified. The precertified RF modules must still be tested by the local RF authorities, but the level of testing and the risk and cost of the testing are reduced.

### Location of devices

With a wireless product, the location of the product is very important. A wireless product mounted inside a metallic cabinet offers poor range, but a wireless product mounted on the side of the metallic cabinet provides good range except from the backside of the product.

### Battery supply and replacement

Battery-supplied sensors require a certain amount of human intervention to replace batteries, but, with modern, high-capacity batteries and the low-current consumption of mesh network radios, battery life can be counted in multiple years. Depending on the application requirements and the battery type selected, up to 10 years can expected. And the product can be designed to report its battery state so that the battery can be replaced at optimum times for energy consumption and convenience. Further, when maintenance is conducted on the entire building automation system, replacing a battery in a sensor is easy. Energy-harvesting technology can eliminate the need for battery replacement by charging the battery of the product with energy harvested from its surroundings, for example, the light energy collected using a “solar cell” on the product.

Some guesswork may be involved when installing wireless networks. The RF energy is not visible in the same way a set of wires drawn on a blueprint is. But with experience, knowledge of the RF qualities of the products used in the network, and the understanding that an additional, unplanned repeater may be required to obtain stable and secure communication throughout the network, the overall installation effort is significantly less than that of a similar wired network. Monitoring tools and the use of network operation data can also help with wireless network installation. Such tools could, for example, allow the installer to see the amount of RF energy received by the individual devices in the network during network operation. If a device is receiving RF messages below a certain threshold, the mounting location of this device could be adjusted or a repeater could be incorporated in the network to ensure a better RF connection with the device.

Today, no one disputes the advantages of the wireless data networks provided by Wi-Fi, and soon the same will be the case for wireless building automation systems.

With mesh network RF protocols, the low-power consumption of radio systems, and precertified RF modules featuring built-in antennas, the designers and users of building automation systems are experiencing a paradigm shift.

## What Wireless Solutions does Silicon Labs Offer for Building Automation?

Silicon Labs empowers device makers to capitalize on this revenue opportunity, as more building managers enter the era of wireless technology. Our industry leading wireless chipsets and modules, accompanied by software and development tools, enable secure and robust connectivity across fragmented, multiprotocol smart building environments.

With Silicon Labs, you can enable smart building devices with the broadest selection of hardware, innovative wireless software, and the most robust security with technology support for Zigbee, EnOcean, Wi-Fi, and Bluetooth protocols.

Uncover the Silicon Labs Wireless Solutions for Smart Buildings

Learn More